岡山理科大学紀要 第39号 A pp. 27-33(2003)

循環小数と素体の乗法群について

高嶋 惠三 ・ 内藤 有里*

岡山理科大学理学部応用数学科

〒700-0005 岡山市理大町 1 -1

* 倉敷市立新田中学校

〒710-0038 倉敷市新田 2674-3

(2003年11月 7 日 受理)

1 背景と主結果

よく知られているように、 10 進法のもとで素数 p $((10,p)=1)$ に対して、$\frac{1}{p}$ は循環小数になる。ここで、 (a,b) は整数 a , b の最大公約数である。これに関連して多くの結果が知られているが、循環の周期に関しては以下の結果が重要である :

定理 A ([1]) 正の整数 n , $(n,10)=1$, に対して $\frac{1}{n}$ は循環小数となり、その周期は $10^e \equiv 1 \pmod{n}$ を満たす、最小の正の指数 e である。

特に n がある種の素数、例えば $p=23$ に対しては、$\frac{1}{p}$ は最長周期 $p-1$ 桁を持ち、

$$\frac{1}{p} = 0.\dot{0}434782608695652173913\dot{}$$

となり、 22 $(=p-1)$ 桁の周期で循環する。この時、循環部分の前半と後半を足すと、

$$04347826086 + 95652173913 = 99999999999$$

のように、 $9(=10-1)$ が並ぶことになる。ここで、$\dot{0}$, $\dot{3}$ は循環する部分の初めと終りを表す。

本報告では、この事実をさらに一般化して、 m 進法のもとで素数 p $(p \nmid m)$ について、その逆数 $\frac{1}{p}$ がどのような循環小数となるか、について素体 $GF(p)$ の乗法群 $GF(p)^+ = \{1,2,\ldots,p-1\}$ との関係を踏まえて議論し以下の結果を示す :

定理 1 奇素数 p と正の整数 m に対し、$m^k \equiv p-1 \pmod{p}$ を満たす正の整数 k が存在する場合、$\frac{1}{p}$ は

$$\frac{1}{p} = 0.\dot{a_1}a_2\cdots\dot{a}_{2k}, \quad (\ m \text{ 進法 }\ )$$

のように長さ $2k$ で循環する小数に展開され、$a_i + a_{k+i} = m-1, i=1,\ldots,k,$ が成り立つ。

注意 上記の定理の $2k$ は必ずしも $\frac{1}{p}$ の循環の周期、とは限らない。例えば、$m=6$, $p=7$ の場合、$6^3 \equiv 6 \pmod{7}$ であり、実際 6 進法で $\frac{1}{7} = 0.\dot{0}50505\dot{}$ となり、 $0+5=5$, $5+0=5$, $0+5=5$ が成り立つ。この場合、循環の周期は 2 であり、 $6^2 \equiv 1 \pmod{7}$ が成り立つ。また、素数 2 に対しては上記のような結果は成り立たない。何故なら、 $p-1=1$ であるから。また、こ

の定理より $m^k \equiv p-1 \pmod p$ が確認される場合、$\frac{1}{p}$ の計算をする場合に循環する部分の前半の k 桁を計算すれば残りの k 桁は自動的に決定されることが分かる。

2 素体 $GF(p)$ とその乗法群

この節では、定理の証明に入る前に素体の乗法群について簡単にまとめておく。

よく知られているように、素数 p に対して、$GF(p)=\{0,1,\ldots,p-1\}$ は p を法とする加法と乗法に関して体をなす。また、$GF(p)^+ = GF(p)\setminus\{0\}$ とおくと、$GF(p)^+$ は乗法に関して群をなし、巡回群になることも周知の事実である：

定理 B ([2]) 有限体 F には少なくとも一つの原始元 α が存在し、乗法群 $F^+ = F\setminus\{0\}$ は α を生成元とする巡回群を構成する。

奇素数 p を考える。$GF(p)^+$ の位数は $p-1$ で偶数であるから、$p-1 = 2^{e_0}p_1^{e_1}\cdots p_r^{e_r}$ と因数分解される場合、Abel 群の基本定理より巡回群の直積に分解される：

$$GF(p)^+ = G_0 \otimes G_1 \otimes \cdots \otimes G_r ,$$

ここで、G_0 は位数 2^{e_0} の巡回群であり、G_j は位数 $p_j^{e_j}$ $j=1,\ldots,r$ の巡回群である。g_j を G_j の生成元とすると、$g_0g_1\cdots g_r$ は $GF(p)^+$ の生成元、すなわち $GF(p)$ の原始元である。また、$p-1$ は $GF(p)^+$ の唯一の位数 2 の元であることも容易に分かる。

3 定理 1 の証明と簡単な結果

定理 1 の証明 まず、$m>p$ の場合には、$m\equiv m' \pmod p$ を考えることにより、$m'^k \equiv m^k \pmod p$ であることに注意すると、定理の証明は $m<p$ の場合に考えればよいことが分かる。

定理の条件より、$m^k \equiv p-1 \pmod p$ であり、$(p-1)^2 \equiv 1 \pmod p$ であるから、明らかに $m^{2k}\equiv 1 \pmod p$ となり、定理 A の一般化より $\frac{1}{p}$ は m 進法で長さ $2k$ の循環小数で表されることが分かる。

次に、$m^k = Ap+p-1$, と表されるとすると $(p-1)m^k = Bp+1$, と表されることが分かる。この両式の両辺どうしを足しあわせると $pm^k = (A+B)p+p$, となり、両辺を p で割って $m^k-1 = A+B$, を得る。A が $\frac{1}{p}$ の m 進法での前半の k 桁, $a_1\cdots a_k$, であり、B が後半の k 桁, $a_{k+1}\cdots a_{2k}$, であることを考えると定理の結論が証明されたことになる。また、各桁 a_i は $m-1$ 以下の数であるから、$A+B$ の計算は各桁毎の足し算に等しいことも明らかである。

(証明終)

この定理から容易に以下の結果を得る。

系 1 $m\in GF(p)^+$ の位数が ℓ の場合、$m^\ell \equiv 1 \pmod p$ が一般に成り立つので、m 進法での $\frac{1}{p}$ の循環小数の周期は ℓ である。ℓ が偶数の場合、$m^{\frac{\ell}{2}} \equiv p-1 \pmod p$, が成り立ち、$m$ 進法での $\frac{1}{p}$ の小数展開について定理の結果が成り立つ。

また、ℓ が奇数の場合には $m^{\frac{\ell}{2}} \not\equiv p-1 \pmod p$, となるので、定理の結果のような循環小数表現を持つことはない。

証明　巡回群 $GF(p)^+$ の位数 2 の元は $p-1$ のみであるから、$m^{\frac{\ell}{2}} \equiv p-1 \pmod{p}$ となり、定理の条件が満たされる。

(証明終)

次に、前節で述べたように、$GF(p)^+ = G_0 \otimes G_1 \otimes \cdots \otimes G_r$, と分解される場合、$G_1 \otimes \cdots \otimes G_r$, の元の位数は奇数であるので、$m$ がこの部分群の元である場合には、定理の結果のような循環小数表現を持たない。

系 2　$m = p-1$ の場合、m 進法では $\frac{1}{p} = 0.\dot{0}\dot{m}'$ $(m' = m-1)$, となる。また、$m = p+1$ の場合、m 進法では $\frac{1}{p} = 0.\dot{1}$ と表される。

系 3　$GF(p)^+$ で m が偶位数 2ℓ を持つ場合、$\frac{1}{p}$ の m 進法での展開の前半の ℓ 桁と後半の ℓ 桁を入れ替えると、$\frac{p-1}{p}$ の m 進法での展開が得られる。

さらに、m から生成される巡回部分群 $< m >$ の元 m^k に対して、$\frac{m^k}{p}$ の循環小数表現 (m 進法) は、$\frac{1}{p}$ の循環小数表現の小数部分が循環したものとなる。

証明　定理 1 の証明で見たように、$m^\ell = Ap + p - 1$, と表すと、A が m 進法での展開の前半になる。一方、$(p-1)m^\ell = Bp + 1$, とすると、B は展開の後半になるが、同時に $\frac{p-1}{p}$ の m 進法での展開の前半でもある。このことから、系の結果が得られる。後半の結果は $\frac{1}{p}$ の小数の計算から明らかである。

(証明終)

これらの議論から明らかなように、$\frac{1}{p}$ の m 進法での小数展開を調べることにより、$GF(p)^+$ の乗法群としての構造を決めることが出来ることが分かる。

4　具体例

この節では、いくつかの奇素数 p について具体的に m 進法での $\frac{1}{p}$ の表現を示し、m の位数との関連を示す。

例 1　$p = 7$ の場合。$p - 1 = 6 = 2 \times 3$ であるから、$GF(7)^+ = G_0 \otimes G_1$,　$G_0 = \{1, 6\}$, $G_1 = \{1, 2, 4\}$, と分解される。従って、原始根は $6 \times 2 \equiv 5 \pmod{7}$, $6 \times 4 \equiv 3 \pmod{7}$, であり、

$$\frac{1}{7} = 0.\dot{0}10212\dot{}, \quad (3 \text{ 進法}), \quad \frac{1}{7} = 0.\dot{0}32412\dot{}, \quad (5 \text{ 進法}),$$

となる。さらに、例えば $m = 3$ の場合、$< 3 >= \{1, 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5\}$ であるから、3 進法では

$$\frac{3}{7} = 0.\dot{1}02120\dot{}, \quad \frac{2}{7} = 0.\dot{0}21201\dot{}, \quad \frac{6}{7} = 0.\dot{2}12010\dot{}, \quad \frac{4}{7} = 0.\dot{1}20102\dot{}, \quad \frac{5}{7} = 0.\dot{2}01021\dot{},$$

となり、定理と系 3 の結果が成り立つことが分かる。但し、便宜上、分数の分子、分母の数は 10 進法で表した。

一方、 $m=2,4$ の場合には位数は3であるので、

$$\frac{1}{7}=0.\dot{0}0\dot{1}, \quad (2 \text{ 進法}) \ , \frac{1}{7}=0.\dot{0}2\dot{1}, \quad (4 \text{ 進法}),$$

となる。また、明らかに $\frac{1}{7}=0.\dot{0}\dot{5}$, (6 進法), である。さらに、 $m>7$ の場合には、例えば $m=10\equiv 3 \pmod 7$ の場合には 3 進法と同様に $\frac{1}{7}=0.\dot{1}42857$, (10 進法), となり、定理の結果が成り立つ。

例 2 $p=5$ の場合。 $p-1=4=2^2$ であるから、$GF(5)^+$ は位数 4 の巡回群となる。実際、$GF(5)^+=\{1,2,2^2=4,2^3=3\}$ であり、原始根は 2 と 3 である。 $m=2$ の場合、

$$\frac{1}{5}=0.\dot{0}0\dot{1}\dot{1}, \ \frac{2}{5}=0.\dot{0}\dot{1}1\dot{0}, \ \frac{4}{5}=0.\dot{1}\dot{1}0\dot{0}, \ \frac{3}{5}=0.\dot{1}0\dot{0}\dot{1},$$

となり、定理と系 3 の結果が成り立つ。また、

$$\frac{1}{5}=0.\dot{0}12\dot{1}, \ (3 \text{ 進法}) \ \frac{1}{5}=0.\dot{0}\dot{3}, \ (4 \text{ 進法}).$$

例 3 $p=13$ の場合。$p-1=12=2^2\times 3$ であり、$GF(13)^+=G_0\otimes G_1=\{1,5,8,12\}\otimes\{1,3,9\}$ と分解される。これより原始根は $5\times 3\equiv 2 \pmod{13}$, $5\times 9\equiv 6 \pmod{13}$, $8\times 3\equiv 11 \pmod{13}$, $8\times 9\equiv 7 \pmod{13}$, である。

$$\frac{1}{13}=0.\dot{0}00100111101\dot{1}, \ (2 \text{ 進法}), \ \frac{1}{13}=0.\dot{0}24340531215\dot{5}, \ (6 \text{ 進法}),$$

$$\frac{1}{13}=0.\dot{0}35245631421\dot{3}, \ (7 \text{ 進法}), \ \frac{1}{13}=0.\dot{0}93425A1768\dot{5}, \ (11 \text{ 進法}),$$

となる。但し、 10 以上（ 10 進法で）の数を表すのに $A=10, B=11, C=12$, 等の表現を用いることにする。

一方、 $m=4,10$ は位数 6 であり、

$$\frac{1}{13}=0.\dot{0}1032\dot{3}, \ (4 \text{ 進法}), \ \frac{1}{13}=0.\dot{0}7692\dot{3}, \ (10 \text{ 進法}),$$

となる。例えば 4 進法の場合、$<4>=\{1,4,3,12,9,10\}$ であることに注意すると、

$$\frac{1}{13}=0.\dot{0}1032\dot{3}, \ \frac{4}{13}=0.\dot{1}0323\dot{0}, \ \frac{3}{13}=0.\dot{0}3230\dot{1},$$

$$\frac{12}{13}=0.\dot{3}2301\dot{0}, \ \frac{9}{13}=0.\dot{2}3010\dot{3}, \ \frac{10}{13}=0.\dot{3}0103\dot{2},$$

となり、系 3 の結果が成り立つことが分かる。また、 $m=5,8$ は位数 4 であり、

$$\frac{1}{13}=0.\dot{0}14\dot{3}, \ (5 \text{ 進法}), \ \frac{1}{13}=0.\dot{0}47\dot{3}, \ (8 \text{ 進法}),$$

となり、定理の結果が成り立つ。一方、 $m=3,9$ は位数 3 であり、

$$\frac{1}{13}=0.\dot{0}0\dot{2}, \ (3 \text{ 進法}), \ \frac{1}{13}=0.\dot{0}6\dot{2}, \ (9 \text{ 進法}),$$

となり、定理の形の小数表現は持たないことが分かる。

例 4 $p=17$ の場合。$p-1=2^4\times 3$ であり、$p=5$ の場合と同様に、$GF(17)^+$ の 1 以外の元の位数はすべて偶数であり、定理と系 3 の結果が成り立つ。原始根は $m=3,5,6,7,10,11,12,14$ である。これらに対しては以下の結果を得る：

$$\frac{1}{17}=0.\dot{0}011202122111020\dot{1},\ (3\text{ 進法}),\quad \frac{1}{17}=0.\dot{0}121340243231042\dot{2},\ (5\text{ 進法}),$$

$$\frac{1}{17}=0.\dot{0}204122453514331\dot{3},\ (6\text{ 進法}),\quad \frac{1}{17}=0.\dot{0}261143464055232\dot{2},\ (7\text{ 進法}),$$

$$\frac{1}{17}=0.\dot{0}588235294117647\dot{7},\ (10\text{ 進法}),\quad \frac{1}{17}=0.\dot{0}7132651A3978459\dot{9},\ (11\text{ 進法}),$$

$$\frac{1}{17}=0.\dot{0}8579214B36429A\dot{7},\ (12\text{ 進法}),\quad \frac{1}{17}=0.\dot{0}B75A9C4D2683419\dot{9},\ (14\text{ 進法}).$$

また、$m=2,8,9$ の位数は 8 であり、

$$\frac{1}{17}=0.\dot{0}000111\dot{1},\ (2\text{ 進法}),\quad \frac{1}{17}=0.\dot{0}3607417\dot{7},\ (8\text{ 進法}),\quad \frac{1}{17}=0.\dot{0}467842\dot{1},\ (9\text{ 進法}).$$

$m=4,13$ は位数 4 であり、

$$\frac{1}{17}=0.\dot{0}03\dot{3},\ (4\text{ 進法}),\quad \frac{1}{17}=0.\dot{0}9C\dot{3},\ (13\text{ 進法}).$$

例 5 $p=19$ の場合。$p-1=18=2\times 3^2$ であり、

$$GF(31)^+=G_0\otimes G_1=\{1,18\}\otimes\{1,4,5,6,7,9,11,16,17\}$$

と分解され、原始根は $m=2,3,10,13,14,15$ となる。これらに対しては、

$$\frac{1}{19}=0.\dot{0}00011010111100101\dot{1},\ (2\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}01102100221120122\dot{2},\ (3\text{ 進法}),$$

$$\frac{1}{19}=0.\dot{0}52631578947368421\dot{1},\ (10\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}8B82976AC414A3562\dot{2},\ (13\text{ 進法}),$$

$$\frac{1}{19}=0.\dot{0}A45C7522D398168B\dot{B},\ (14\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}BC9718A3E3257D64\dot{B},\ (15\text{ 進法}),$$

となり、定理の結果が成り立つ。また、$m=8,12$ は位数 6 であり、

$$\frac{1}{19}=0.\dot{0}32745\dot{5},\ (8\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}76B45\dot{5},\ (12\text{ 進法}).$$

これらと $m=18$ 以外の $GF(19)^+$ の元の位数は奇数であるので、定理の結果のような循環小数表現は持たないことは容易に確かめられる。実際、$m=4,5,6,9,16,17$ の位数 9 であり、

$$\frac{1}{19}=0.\dot{0}03113211\dot{1},\ (4\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}11242141\dot{1},\ (5\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}15211325\dot{5},\ (6\text{ 進法}),$$

$$\frac{1}{19}=0.\dot{0}42327188\dot{8},\ (9\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}D79435E5\dot{5},\ (16\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}F39E5648\dot{8},\ (17\text{ 進法}),$$

となる。また、$m=7,11$ の位数は 3 であり、

$$\frac{1}{19}=0.\dot{0}24\dot{4},\ (7\text{ 進法}),\quad \frac{1}{19}=0.\dot{0}64\dot{4},\ (11\text{ 進法}),$$

となる。

例 6 $p=31$ の場合。 $p-1=30=2\times3\times5$ であり、

$$GF(31)^+=G_0\otimes G_1\otimes G_2=\{1,30\}\otimes\{1,5,25\}\otimes\{1,2,4,8,16\}$$

と分解され、原始根は $m=3,11,12,13,17,21,22,24$ となる。これらに対しては、

$$\frac{1}{31}=0.\dot{0}00212111221020222010111001202\dot{},\ (3\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}39A32146818574A71078964292536\dot{},\ (11\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}478AA093598166B74311B28623A55\dot{},\ (12\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}55B42692C21347C7718A63A0AB985\dot{},\ (13\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}9583E469EDC11AG7B8D2CA7234FF6\dot{},\ (17\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}E4FC4179A382EIK6G58GJDBAHCI62\dot{},\ (21\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}FDAE45EJJ3C194L68B7HG722I9KC\dot{H},\ (22\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}IDMAK327HJ8C96N5A1D3KLG64FBE\dot{H},\ (24\text{ 進法}).$$

また、 $m=15,23,27,29$ は位数 10 であり、

$$\frac{1}{31}=0.\dot{0}73D0E7B1\dot{E},\ (15\text{ 進法}),\quad \frac{1}{31}=0.\dot{0}H1B2M5LB\dot{K},\ (23\text{ 進法}),$$

$$\frac{1}{31}=0.\dot{0}NDP6Q3D1\dot{K},\ (27\text{ 進法}),\quad \frac{1}{31}=0.\dot{0}R3LES1P7\dot{E},\ (29\text{ 進法}),$$

また、 $m=6,26$ は位数 6 であり、

$$\frac{1}{31}=0.\dot{0}10545\dot{},\ (6\text{ 進法}),\quad \frac{1}{31}=0.\dot{0}LKP45\dot{},\ (26\text{ 進法}),$$

いずれの場合にも定理の結果が成り立つことが分かる。

これらと $m=30$ 以外の $GF(31)^+$ の元の位数は奇数であるので、定理の結果のような循環小数表現は持たないことは容易に確かめられる。

参考文献

[1] 高木貞治：初等整数論講義（共立出版）

[2] 高橋磐郎：組合せ理論とその応用（岩波）

On Cyclic Fractions and Multiplicative Groups of Prime Fields

Keizo Takashima and Yuri Naito*

Dept. of Applied Mathematics, Okayama Univ. of Science
*1-1, Ridaicho, Okayama 700-0005 Japan * Shinden Junior High School*
2674-3, Shinden, Kurashiki 710-0038 Japan

(Received November 7, 2003)

In this note, we will consider cyclic fractions not only in usual decimal notation system, but also in more general notation systems. We will derive some relations between cyclic fractions and multiplicative groups of prime fields.

Let p be a odd prime. It is well-known that in case 10 is a primitive root of GF(p), and in case 10 has even order ℓ, $\frac{1}{p}$ has a cyclic fraction expression of period ℓ. To see this in detail, let us consider an example: in case of $p = 23$ and decimal notation system,

$$\frac{1}{p} = 0.\dot{0}4347826086956521739\dot{1}\dot{3}$$

and the former part of digits and the latter part have the next relation:

$$04347826086 + 95652173913 = 99999999999.$$

This paper extends this results with considering multiplicative groups of finite prime fields, and our result is as follows.

Theorem Let m be a positive interger, and p be an odd prime number. If there exists an positive integer ℓ, such that $m^\ell \equiv p - 1 \pmod{p}$, then $\frac{1}{p}$ has a cyclic fractional expression in m notation system, with length 2ℓ, as follows,

$$\frac{1}{p} = 0.\dot{a_1}a_2 \ldots a_\ell a_{\ell+1} \ldots a_{2\ell},$$

and it satisfies the following relation:

$$a_1 + a_{\ell+1} = \cdots = a_\ell + a_{2\ell} = m - 1.$$